Computational Algorithms and Numerical Dimensions

www.journal-cand.com

Com. Alg. Num. Dim Vol. 4, No. 2 (2025) 95–105.

Paper Type: Original Article

Exploring Gröbner Bases for Practical Problem-Solving Applications

Hamed Farahani*

Department of Mathematics, Chabahar Maritime University, Chabahar, Iran; hamed.grobner60@gmail.com.

Citation:

Received: 21 November 2024 *Revised: 26 February 2025* *Accepted: 08 April 2025*	Farahani, H. (2025). Exploring Gröbner Bases for Practical Problem-Solving Applications. Computational Algorithms and Numerical Dimensions,4(2), 95-105

Abstract

Gröbner bases serve as a crucial theoretical cornerstone in contemporary (polynomial) ring theory. The development of Gröbner basis theory originated from efforts to address theoretical issues related to ideals in polynomial rings and to solve systems of polynomial equations. This article explores three practical applications of Gröbner basis theory: using Gröbner bases to solve systems of nonlinear polynomial equations, tackling an k-corolability problem, determining the chromatic number of a graph, and presenting a unique example from the automatic geometric proving. By understanding these applications, we can appreciate how Gröbner bases bridge abstract algebraic concepts with tangible computational solutions.

Keywords: Fuzzy numbers, Fuzzy matrices, Gröbner bases, Fuzzy inverse matrix, Fuzzy linear equation systems.

1|Introduction

Gröbner basis theory is a fundamental concept in computational algebra, particularly in the study of polynomial ideals. The history of Gröbner bases can be traced back to the work of Austrian mathematician Wolfgang Gröbner and his student Bruno Buchberger. Although Gröbner himself did not develop the concept, his work in algebraic geometry and ring theory laid important groundwork. The concept of Gröbner bases was named in his honor. The formal development of Gröbner basis theory began with Buchberger's Ph.D. thesis in 1965 at the University of Innsbruck, under the supervision of Wolfgang Gröbner . Buchberger introduced an algorithm (now called the Buchberger algorithm) for constructing a Gröbner basis for a given ideal in a polynomial ring. This algorithm transformed the approach to polynomial equations,

Corresponding Author: farahani@cmu.ac.ir
https://doi.org/10.22105/bdcv.2024.491412.1219

making it easier to perform operations such as ideal membership testing and solving systems of polynomial equations. Buchberger's work marked a major advancement in computational algebra. Gröbner bases provided a systematic method to tackle problems that were previously unsolvable or difficult to handle computationally. The theory found applications in solving polynomial systems, computer algebra systems, and algebraic geometry. Over the years, Gröbner basis theory has been extended and refined. Mathematicians have developed efficient algorithms and explored various applications in fields such as coding theory, robotics, and optimization. Today, Gröbner bases are an essential tool in computer algebra systems like Maple, Mathematica, and Singular.

Gröbner bases are a powerful tool in computational algebra and have a wide range of applications in various fields, including mathematics, computer science, engineering, and beyond [3, 4, 9, 10, 11, 12, 17, 19, 21, 22]. Here is a comprehensive overview of some of the main applications:

(1) **Solving Systems of Polynomial Equations**

- Gröbner bases are used to transform systems of polynomial equations into a simpler form that is easier to solve.
- They provide a method to determine whether a system of equations has solutions and to compute those solutions if they exist.

  Applications:

  - Algebraic geometry for finding intersection points of algebraic varieties.
  - Robotics and kinematics for solving systems related to the movement and configuration of mechanical systems.

(2) **Algebraic Geometry**

- Gröbner bases are fundamental in computational algebraic geometry for studying the properties of varieties.
- They are used to compute:
  - Dimension of an algebraic variety.
  - Hilbert function and series.
  - Radical of an ideal, which helps to find the underlying geometric object.
- They also play a crucial role in the elimination theory, which helps eliminate variables to find the projection of varieties.

(3) **Symbolic Computation and Computer Algebra Systems (CAS)**

- Many computer algebra systems like Mathematica, Maple, and Singular use Gröbner bases for polynomial simplification, solving equations, and ideal operations.
- Gröbner bases help to simplify expressions and perform symbolic integration and differentiation involving polynomials.

(4) **Cryptography**

- Used in algebraic attacks on cryptographic systems.
- Gröbner basis techniques can be applied to solve systems of polynomial equations derived from cryptographic protocols, especially in multivariate public key cryptosystems.
- Helps analyze the security of cryptographic schemes, particularly in post-quantum cryptography.

(5) **Coding Theory**

- In the design and analysis of error-correcting codes, Gröbner bases are used to analyze and construct algebraic codes.
- They help in decoding algorithms for certain types of codes, like cyclic codes and Reed-Solomon codes, using algebraic techniques.

(6) **Robotics and Kinematics**

- Used to model and solve inverse kinematics problems for robotic arms and other mechanisms.
- Helps in designing paths and understanding the constraints and reachable positions of mechanical systems.
- Applications in computer-aided design (CAD) for movement planning and simulation.

(7) **Combinatorial Optimization**

- Gröbner bases are used to solve problems in integer programming and combinatorial optimization.
- Applications include scheduling, resource allocation, and network design.
- In integer programming, they help in transforming a polynomial optimization problem into a simpler form that can be solved using algebraic techniques.

(8) **Control Theory**

- Applied to the analysis and design of control systems.
- Helps in solving polynomial equations that model the behavior of dynamic systems and in designing controllers for such systems.
- Useful in the analysis of the stability and controllability of nonlinear systems.

(9) **Theoretical Computer Science**

- In complexity theory, Gröbner bases are used to analyze the complexity of algorithms related to polynomial ideals.
- Used in automated theorem proving and formal verification to handle polynomial expressions that arise in logical proofs.

(10) **Computational Biology and Bioinformatics**

- Used in modeling biochemical networks and analyzing polynomial dynamical systems.
- Helps in understanding gene regulatory networks and metabolic pathways by solving systems of polynomial equations that describe the interactions in biological systems.

(11) **Number Theory**

- Gröbner bases help in solving Diophantine equations (polynomial equations with integer coefficients).
- Applications include studying integer solutions to polynomial equations and in algebraic number theory.

(12) **Chemistry and Physics**

- In quantum chemistry and physics, they are used to solve polynomial equations that describe molecular structures and energy states.
- Used in modeling and simulating physical systems with polynomial constraints, such as equilibrium states in chemical reactions.

(13) **Mechanics and Structural Engineering**

- Applied to problems involving the equilibrium and deformation of structures.
- Helps in analyzing stress and strain in mechanical systems by solving equations derived from physical constraints.

(14) **Algorithmic Applications**

- Gröbner basis algorithms, such as Buchberger's algorithm, are widely studied and applied in algorithmic research to develop efficient techniques for solving polynomial equations.
- These algorithms have broad applications in the development of software for scientific computation and engineering analysis.

(15) **Artificial Intelligence and Machine Learning**

- Emerging applications in AI/ML involve Gröbner bases for feature selection and in the analysis of polynomial-based models.
- They can be used to understand the structure of decision boundaries in polynomial classifiers.

(16) **Algebraic Statistics**

- Used in the field of algebraic statistics for maximum likelihood estimation and to study statistical models that are described by polynomial equations.
- Applications include the analysis of contingency tables and the design of experiments.

Gröbner bases thus provide a unifying framework for tackling a wide variety of problems that involve polynomial equations, both in pure mathematics and applied sciences. Their computational efficiency and theoretical depth make them a crucial tool in many areas of research and industry.

2|Gröbner basis background

Bruno Buchberger in his 1965 PhD thesis was originally presented the concept of Gröbner basis for overcomming the challenge of the ideal membership problem for polynomials ring over a field. Next, he introduced Buchberger's algorithm [2] for obtaining the Gröbner basis for an polynomial ideal. Among all available efforts to improve this algorithm, F_4 and F_5 algorithms presented in [13, 14], are the most efficient algorithms.

In this subsection aims to devote the basic concepts and statements on Gröbner basis. Next, a brief exposition of Buchberger's algorithm is presented. Polynomial equations systems in a very nice fashion can be resolved using Gröbner basis method.

The polynomial ring in the set of variables $x_1, ..., x_n$ with coefficients in field $\mathbb{K}$ is called a polynomial ring. It is denoted by $\mathcal{K}[\mathbf{x}] = \mathbb{K}[x_1, ..., x_n]$. An expression of the form $x_1^{r_1} x_2^{r_2} ... x_n^{r_n}$ for non-negative integers $r_1, ..., r_n$ is said to be monomial. It should be noted that a monomial order is an essential tool to define a Gröbner basis.

Definition 0.1. *Let $\theta = (\theta_1, ...\theta_n)$ and $\sigma = (\sigma_1, ..., \sigma_n)$ are two n- tuples in $\mathbb{Z}^n_{\geq 0}$. We will have $\theta \succ_{lex} \sigma$ if $\theta - \sigma \in \mathbb{Z}^n$, the leftmost nonzero entry is positive. It may be written $\theta \succ_{lex} \sigma$ when $x_1^{\theta_1} x_2^{\theta_2} ... x_n^{\theta_n} \succ_{lex} x_1^{\sigma_1} x_2^{\sigma_2} ... x_n^{\sigma_n}$.*

For a fixed monomial order, the largest monomial appearing in non-zero polynomial f with respect to (w.r.t.) $\succ$ is indicated by $\mathcal{LT}(f)$, and is said to be the leading term of f. The coefficient of $\mathcal{LT}(f)$ is the leading coefficient of f is indicated by $\mathcal{LC}(f)$.

Definition 0.2. *Consider the ideal $I = \langle f_1, \ldots, f_m \rangle$ in $\mathcal{K}[\boldsymbol{x}]$ (denoted as $I \trianglelefteq \mathcal{K}[\boldsymbol{x}]$). For a specified ordering, we define $\mathcal{LT}(I) = \mathcal{LT}(f) : f \in I$. The ideal generated by the elements of $\mathcal{LT}(I)$ is represented by $\langle \mathcal{LT}(I) \rangle$.*

Now, for an ideal in $\mathcal{K}[\mathbf{x}]$ a Gröbner can be defined as follows:

Definition 0.3. *Let a monomial order $\succ$ has been fixed. A Gröbner basis for the ideal I in $\mathcal{K}[\boldsymbol{x}]$, w.r.t. $\succ$ is a finite polynomials set $G = \{g_1, g_2, ..., g_m\}$ with the following properties:*

- ***Generating the Ideal*** *the ideal generated by* $g_1, g_2, ..., g_m$ *will be* $I = \langle g_1, g_2, ..., g_m \rangle$.
- ***Reduction Property*** *for any polynomial* $f \in I$, *the division algorithm ensures that the reminder of* f *when divided by the polynomials* $g_1, g_2, ..., g_m$ *is zero. this means that the leading term of* f *can be reduced using the leading term of the* g_i.

In the other words, if f *is in the ideal* I, *then there exist unique polynomials* $q_1, q_2, ..., q_m$ *in* $\mathcal{K}[\boldsymbol{x}]$ *such that* $f = g_1q_1 + g_2q_2 + ... + g_mq_m + r$ *where* r *is the reminder and for all* i, *we have* $\mathcal{LT}(r) < \mathcal{LT}(g_i)$.

Buchberger's Algorithm takes a set of polynomials $\{f_1, f_2..., f_m\}$ that generate an ideal I in a polynomial ring $\mathcal{K}[\mathbf{x}]$ and computes a Gröbner basis G for I. This basis has desirable properties, such as making ideal membership tests and solving systems of polynomial equations more straightforward.

Definition 0.4. *The* S*-polynomial of two polynomials* f *and* g *is defined to help eliminate leading terms:*

$$S(f, g) = \frac{\mathcal{LCM}(\mathcal{LT}(f), \mathcal{LT}(g))}{\mathcal{LT}(f)} \cdot f - \frac{\mathcal{LCM}(\mathcal{LT}(f), \mathcal{LT}(g))}{\mathcal{LT}(g)} \cdot g,$$

where $\mathcal{LCM}$ *is the least common multiple of the leading terms.*

Algorithm 0.5. [8] ***(Buchberger's Algorithm Steps)***

- ***Initialization:*** *Start with a set* $G = \{f_1, f_2, \dots, f_m\}$ *of polynomials that generate the ideal* I.
- ***Construct Pairs:*** *Create a set of all pairs* (f_i, f_j) *from* G *where* $i < j$.
- ***Compute S-Polynomials:***
  - *For each pair* (f_i, f_j), *compute the S-polynomial* $S(f_i, f_j)$.
- ***Reduce the S-Polynomial:***
  - *Reduce* $S(f_i, f_j)$ *modulo* G *(using polynomial division). If the reduced S-polynomial is non-zero, add it to* G *and update the set of pairs to include new combinations with this new polynomial.*
- ***Repeat:***
  - *Continue computing and reducing S-polynomials until all pairs yield S-polynomials that reduce to zero.*
- ***Termination:*** *When no new non-zero polynomials are added to* G, *the algorithm terminates, and* G *is a Gröbner basis for the ideal.*

The remainder r in Definition (0.3) can be considered a canonical representative of its cosets $[f] \in \Gamma$, where $\Gamma = \frac{\mathcal{K}[\mathbf{x}]}{I}$. These remainders are expressed as linear combinations of the monomials x^α where $x^\alpha \notin \mathcal{LT}(I)$. This collection of monomials is a linearly independent subset of Γ, thus it can be regarded as a basis for Γ. In other words, the set of monomials

$$\Lambda = \{x^\alpha : x^\alpha \notin \mathcal{LT}(I)\}$$

forms a basis for Γ. more specifically, the cosets of these monomials form a basis. This set Λ is called the set of standard monomials.

Proposition 0.6. *Let* $I \subset \mathbb{C}[\boldsymbol{x}]$ *be an ideal, define* $\Omega = \frac{\mathbb{C}[\boldsymbol{x}]}{I}$, *and consider the finite set* $V = V(I)$. *Then*

(1) *The number of elements in* V *is at most* $\dim(\Omega)$ *(where 'dim' indicates the dimension over the vector space* $\mathbb{C}$*).*

(2) *If* I *is a radical ideal, then the number of elements in* V *is equal to* $\dim(\Omega)$*), meaning* $|V| = \dim(\Omega)$.

Definition 0.7. *A reduced basis for the ideal I in $\mathcal{K}[\boldsymbol{x}]$ is a Gröbner basis with the additional properties that enhance its usefulness. Specially, a reduced Gröbner basis satisfies the following conditions:*

- ***Generating the Ideal*** *Like any Gröbner basis, it generates the same ideal I.*
- ***Leading Coefficients*** *The leading coefficient of each polynomial in the basis is 1 (normalized).*
- ***Reduction Property*** *For each polynomial g_i in the basis, there is no polynomial in the basis such that $\mathcal{LT}(g_i)$ divides $\mathcal{LT}(g_j)$ for any $i \neq j$. This ensures that the leading term of each polynomial does not overlap with the leading terms of others.*

Definition 0.8. *An affine variety is a subset of affine space $\mathbb{A}^n$ defined as the common zeroes of a set of polynomials. Formally, an affine variety $V(I)$ associated with the ideal $I \subset \mathcal{K}[\boldsymbol{x}]$ is given by:*

$$V(I) = \{(t \in \mathbb{K}^n : h(t) = 0 \ \ \forall h \in I\}$$

where $t = (t_1, ..., t_n)$ is a point in $\mathbb{K}^n$.

3|Nonlinear Polynomial Equations Systems and Gröbner basis

Using Gröbner bases allowed us to systematically simplify and solve the polynomial equations systems. This method is powerful for finding solutions of polynomial equations systems, especially in higher dimensional, as it can simplify the problem significantly.

$$\begin{cases} f_1(x_1, x_2, ..., x_n) = 0, \\ \vdots \\ f_k(x_1, x_2, ..., x_n) = 0, \\ \vdots \\ f_m(x_1, x_2, ..., x_n) = 0, \end{cases} \tag{1}$$

where $x_1, x_2, ..., x_n \in \mathbb{R}$.

Affin variety are fundamental objects in algebraic geometry, representing solution to polynomial equations systems in a coordinate space. They can be defined in various way, including as the set of common roots of polynomial algebraic sets corresponding to ideals in the polynomial ring.

The following result presents the main characteristics of Gröbner basis.

Theorem 0.9. *Let $\mathbb{K} \subseteq \mathbb{C}$ and $I = \langle g_1, g_2, ..., g_m \rangle \subset \mathcal{K}[\boldsymbol{x}]$.*

(1) ***Uniqueness*** *For a given ideal and a chosen monomial order, the reduced Gröbner basis is unique.*

(2) ***Ideal Generation*** *The ideal generated by a Gröbner basis is the same as the original ideal I.*

(3) ***Solving Systems*** *Gröbner bases can simplify solving system of polynomial equations, often transforming the problem into a simple form (e.g., triangular form).*

As a result, in any extending field of $\mathbb{K}$, there is no solution for the equations $g_1 = 0, ..., g_m = 0$ if and only if $G = \{1\}$.

(4) ***Dimension and Variety*** *The dimension of affine variety corresponding to I can be determined using Gröbner basis.*

In actual practice, $V(I) \subset \mathbb{C}^n$ is a finite set $\iff$ for every variable x_1, there exists $g \in G$ so that $LT(g)$ is a power of x_i (I is a zero-dimensional ideal). Notice also that $V(G) = V(g_1, ..., g_m)$.

Then, we compute a Gröbner basis for the ideal generated by it in $\mathbb{R}[x_1, ..., x_n]$. The Gröbner basis w.r.t. the lexicographical order has the upper triangular structure; i.e., it has the following form:

$$\begin{cases} g_{1,1}(x_n) \in \mathbb{R}[x_n], \\ g_{2,1}(x_{n-1}, x_n), ..., g_{2,p_2}(x_{n-1}, x_n) \in \mathbb{R}[x_{n-1}, x_n], \\ \vdots \\ g_{n,1}(x_1, ..., x_{n-1}, t_n), ..., g_{n,p_n}(x_1, ..., x_{n-1}, x_n) \in \mathbb{R}[x_1, ..., x_n], \end{cases} \tag{2}$$

Because of the fact that the solution set of the above system is finite in $\mathbb{R}[x_1, ..., x_n]$ w.r.t. the lexicographical order, we can find the solutions of the above system by applying the forward substitutions.

Example 0.10. *Consider the nonlinear polynomial system*

$$f_1 = x^2 + yz + x = 0, \quad f_2 = z^2 + xy + z = 0, \quad f_3 = y^2 + xz + y = 0.$$

We want to find all the solutions (x, y, z) for this system using Gröbner bases. We form the ideal $I = \langle x^2 + yz + x, z^2 + xy + z, y^2 + xz + y \rangle$ generated by the polynomials. Using an algorithm such as Buchberger's algorithm, we compute a Gröbner basis for the ideal I with respect to the lexicographic order ($x \succ_{lex} y \succ_{lex} z$). Let's say we use a computer algebra system (e.g., Mathematica, Maple, or SymPy in Python) to compute the Gröbner basis G. The resulting basis might look like:

$G = \{z^2 + 3z^3 + 2z^4, z^2 + 2yz^2 + z^3 + 2yz^3, y + y^2 - z - yz - z^2 - 2yz^2, z + xz + yz + z^2 + 2yz^2, x + x^2 + yz\}.$

Since the first polynomial depends solely on z, z must be $0, -\frac{1}{2}$ or -1. The system clearly has a finite number of solutions because the third polynomial in G involves only z and y, with its leading term being y^2. Furthermore, the last polynomial includes x, y, and z, with the leading term x^2. If $z = 0$, the system simplifies to $y + y^2 = 0$, $x^3 = 0$, and $x + x^2 = 0$. The simplified set of polynomials is already a reduced Gröbner basis for the ideal it defines. The solutions here are $y = 0$ and $x = 0$ or $x = -1$ and $y = -1$, yielding solutions $(0, 0, 0), (-1, 0, 0)$, and $(0, -1, 0)$. Similarly, for $z = -1$, we have $y^2 = 0$, $-x + y = 0$, $x^3 = 0$, and $x + x^2 - y = 0$. The corresponding reduced Gröbner basis is $\{y, x\}$, giving $x = y = 0$. Thus, another solution is $(0, 0, -1)$. For $z = -\frac{1}{2}$, the reduced Gröbner basis becomes $\{2y + 1, 2x + 1\}$, resulting in the final solution $(-\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2})$.

4|The k-Colorability Problem Using Gröbner Bases

The k-colorability problem is a core issue in graph theory, inquiring whether the vertices of a graph can be assigned k colors in such a way that no two adjacent vertices have the same color. Gröbner bases provide a structured algebraic method for solving this problem [1, 15, 16, 17, 20].

Assume we want to determine if a graph $G = (V, E)$ is k-colorable, and let $n = |V|$. We define the k-coloring ideal $I_k(G) \subset \mathbb{C}[\mathbf{x}]$, which is generated by the vertex polynomials $v_i := x_i^k - 1$, for $1 \leq i \leq n$, and the edge polynomials.

$$\eta_{ij} := \sum_{d=0}^{k-1} x_i^{k-1-d} x_j^d \quad \text{for } \{i, j\} \in E(G).$$

Lemma 0.11. [5] *Consider a graph G with n vertices, and let $I_k(G)$ denote the ideal in $\mathbb{C}[\boldsymbol{x}]$ that is defined by*

$$I_k(G) = \left\langle x_1^k - 1, \ldots, x_n^k - 1, \sum_{d=0}^{k-1} x_i^{k-1-d} x_j^d \right\rangle_{\{i,j\} \in E(G)}.$$

Then, $I_k(G)$ is radical and $\dim\left(\frac{\mathbb{C}[\boldsymbol{x}]}{I_k(G)}\right)$ *is equal to the number of points in $V(I_k(G))$.*

The following theorem, presented by Bayer, states a relation between k-colorability and solvability of polynomial equation systems.

Theorem 0.12. [7] *(Bayer's Theorem) graph G is k-colorable if and only if the following zero-dimensional polynomial equation system has a solution in $\mathbb{C}$. In other words, G is k-colorable if and only if $I_k(G) \neq \langle 1 \rangle = \mathbb{C}[\boldsymbol{x}]$. Furthermore, the number of solutions will be $k!$ times the number of different k-colorings. The number of distinct k-colorings is equal to* $\frac{|V(I_k(G))|}{k!}$.

Example 0.13. *Consider a graph with four vertices $V = \{v_1, v_2, v_3\}$ and edges*

$$E = \{(v_1, v_2), (v_2, v_3), (v_3, v_1)\}.$$

We want to determine if this graph is 3-colorable.

We will assign a variable x_i to each vertex v_i for $i = 1, 2, 3$. For each edge in the graph, we need to ensure that the connected vertices do not have the same color. This gives us the following polynomial constraints:

$$\begin{aligned} x_1^2 + x_1x_2 + x_2^2 &= 0 \quad \textit{(for edge } (v_1, v_2)\textit{)} \\ x_1^2 + x_1x_3 + x_3^2 &= 0 \quad \textit{(for edge } (v_3, v_2)\textit{)} \\ x_2^2 + x_2x_3 + x_3^2 &= 0 \quad \textit{(for edge } (v_3, v_1)\textit{).} \end{aligned}$$

Each variable must take a value in the set $\{0, 1, 2\}$:

$$\begin{aligned} x_1^3 - 1 &= 0 \\ x_2^3 - 1 &= 0 \\ x_3^3 - 1 &= 0. \end{aligned}$$

Let $I_3(G)$ be the ideal generated by the above six polynomials. Then we compute the Gröbner basis of the ideal $I_3(G)$. By using the Maple software, we obtain the reduced Gröbner basis $G^{'}$ of $I_3(G)$ with respect to the lexicographic order:

$$G^{'} = \{x_3^3 - 1, x_2^2 + x_2x_3 + x_3^2, x_1 + x_2 + x_3\}.$$

The reduced Gröbner basis of $I_3(G)$ is not $\{1\}$, then $V(I_3(G) \neq 0$, hence G is 3-colorable by Theorem 3.3. Using Maple, we find that $\dim(C[x_1, x_2, x_3]/I_5(G_\alpha)) = |V(I_3(G)| = 6$. *The number of distinct k-colorings is equal to* $\frac{|V(I_k(G))|}{3!} = \frac{6}{3!} = 1$.

5|Automatic Geometric Theorem Proving using Gröbner Basis

Automatic Geometric Theorem Proving (AGTP) using Gröbner bases is an advanced algebraic technique that allows for the automatic verification of geometric theorems by transforming geometric properties into algebraic conditions. The method provides a systematic approach to determine whether a geometric statement holds by reducing the problem to the study of polynomial equations [6, 18, 23, 24]. Steps in using Gröbner basis for theorem proving is as follows:

1. Model the Geometric Theorem in Algebraic Form:

- Assign coordinates to the geometric entities (such as points, lines, or circles).
- Express the geometric constraints and properties (like collinearity, perpendicularity, and congruence) as polynomial equations. For example, the distance formula, the equation of a circle, or conditions for perpendicular lines.

2. Construct the Ideal:

- Define an ideal I generated by the polynomial equations that represent the given geometric setup. This ideal encompasses all the relationships and constraints dictated by the theorem's premises.

3. Formulate the Theorem Statement:

- Express the theorem you wish to prove as a polynomial equation P. The theorem can be considered true if P is a consequence of the equations defining the ideal I.

4. Compute the Gröbner Basis:

- Use an algorithm, such as Buchberger's algorithm, to compute a Gröbner basis for the ideal I. The Gröbner basis is a set of simpler polynomials that generates the same ideal and facilitates the solution of the system.
- The Gröbner basis provides a canonical representation of the ideal, making it easier to check whether the polynomial P belongs to I.

5. Proof Verification:

- The theorem is proven if P reduces to zero when expressed in terms of the Gröbner basis. This means P can be written as a combination of the polynomials in the Gröbner basis, confirming that P is in the ideal I.

Here's a simple example to illustrate Automatic Geometric Theorem Proving using Gröbner bases for a basic geometric statement:

Theorem 0.14. *The Midpoint of the Hypotenuse of a Right Triangle is Equidistant from the Three Vertices.*

This is a classical result that can be proved using coordinates and Gröbner bases.

Step 1: Set Up the Coordinates. Consider a right triangle with vertices at $A(0,0)$, $B(a,0)$, and $C(0,b)$, where a and b are positive real numbers. The hypotenuse is $\overline{BC}$.

Step 2: Find the Midpoint of the Hypotenuse. The coordinates of the midpoint M of $\overline{BC}$ are:

$$M\left(\frac{a}{2}, \frac{b}{2}\right)$$

Step 3: Formulate the Distance Conditions. To prove the theorem, we need to show that the distances from M to A, B, and C are equal. We express these distances algebraically:

- Distance from M to $A(0,0)$:

$$d_{MA} = \left(\frac{a}{2} - 0\right)^2 + \left(\frac{b}{2} - 0\right)^2 = \frac{a^2}{4} + \frac{b^2}{4} = \frac{a^2 + b^2}{4}.$$

- Distance from M to $B(a,0)$:

$$d_{MB} = \left(\frac{a}{2} - a\right)^2 + \left(\frac{b}{2} - 0\right)^2 = \left(-\frac{a}{2}\right)^2 + \frac{b^2}{4} = \frac{a^2}{4} + \frac{b^2}{4} = \frac{a^2 + b^2}{4}.$$

- Distance from M to $C(0, b)$:

$$d_{MC} = \left(\frac{a}{2} - 0\right)^2 + \left(\frac{b}{2} - b\right)^2 = \frac{a^2}{4} + \left(-\frac{b}{2}\right)^2 = \frac{a^2}{4} + \frac{b^2}{4} = \frac{a^2 + b^2}{4}.$$

Step 4: Set Up Polynomial Equations. We express the conditions $d_{MA} = d_{MB} = d_{MC}$ as a system of polynomial equations:

$$\frac{a^2 + b^2}{4} = \frac{a^2 + b^2}{4} = \frac{a^2 + b^2}{4}$$

(which is always true).

Simplify further to express these equations in terms of polynomial form without radicals:

$$a^2 + b^2 = a^2 + b^2.$$

Step 5: Construct the Ideal and Compute the Gröbner Basis. Using a computer algebra system like Mathematica or Maple, we define an ideal generated by our equations. The Gröbner basis for this ideal will confirm whether our conditions are satisfied.

Step 6: Verify the Theorem If the Gröbner basis simplifies to zero, this indicates that the original equations hold true under the given constraints. In our case, the computations will show that the distances are indeed equal, proving the theorem.

This example demonstrates how we can use coordinates, algebraic expressions, and Gröbner bases to prove geometric theorems automatically. The method verifies that the midpoint of the hypotenuse is equidistant from all three vertices of the right triangle.

6|Conclusion

In this paper, we introduced the concept of Gröbner bases and explored their wide-ranging applications across various domains. Gröbner bases serve as a powerful tool in computational algebra for simplifying and solving systems of polynomial equations. We covered their mathematical theory, key properties, and algorithmic methods, such as Buchberger's algorithm, that enable their computation. Beyond their foundational role in mathematics, we discussed how Gröbner bases contribute to areas such as solving nonlinear polynomial equations system, k-colorability problem, and automatic geometric theorem. This overview emphasizes the practical importance of Gröbner bases in both academic research and industrial applications, showcasing their value in tackling complex algebraic problems effectively.

Acknowledgments

The author would like to express their sincere gratitude to the editors and anonymous reviewers for their invaluable comments and constructive feedback, which significantly contributed to the enhancement of this paper.

Funding

The author declares that no external funding or support was received for the research presented in this paper, including administrative, technical, or in-kind contributions. Data Availability All data supporting the reported findings in this research paper are provided within the manuscript.

Conflicts of Interest

The author declares that there is no conflict of interest concerning the reported research findings. Funders played no role in the study's design, in the collection, analysis, or interpretation of the data, in the writing of the manuscript, or in the decision to publish the results.

References

[1] Al-Anzia, F. S., Sotskov, Y. N., Allahverdi, A., Andreev, G. V. (2006). *Using mixed graph coloring to minimize total completion time in job shop scheduling*, *Applied Mathematics and Computation* , 182(2), 1137–1148.

[2] Buchberger, B. (1985). *Gröbner bases : an algorithmic method in polynomial ideal theory*. R. P. Company, Ed. Bose.

[3] Buchberger, B. (1998). *Applications of Gröbner bases in non-linear computational geometry. In Mathematical aspects of scientific software*, New York, NY: Springer New York.

[4] Buchberger, B., Winkler, F. (1998). *Gröbner bases and applications*, Cambridge University Press.

[5] Cox, D., Little, J., O'Shea, D. (2004). *Using Algebraic Geometry*, second edition. Springer, New York.

[6] Cox, D., Little, J., O'Shea, D. (2007). *Ideal, Varieties, and Algorithms: An introduction to computational algebra geometry and commutative algebra*, third edition. Springer, New York.

[7] De Loera, A., Lee, J., Margulies, S., S. Onn, S. (2009). Expressing combinatorial optimization problems by systems of polynomial equations and the nullstellensatz. *Combinatorics, Probability and Computing* , 18, 551–582.

[8] Dubé, Thomas W. (1990). *The Structure of Polynomial Ideals and Gröbner Bases*, *SIAM Journal on Computing* , 19 (4), 750–773.

[9] Farahani, H., Rahmany, S., Basiri A., Abbasi Molai, A. (2015). *Resolution of a system of fuzzy polynomial equations using eigenvalue method*, *Soft Computing* , 19, 238–291.

[10] Farahani, H., Rahmany, S., Basiri A. (2015). *Determining of level sets for a fuzzy surface using Gröbner basis*, *International Journal of Fuzzy System Applications* , 4(2), 1–14.

[11] Farahmand Nejad, M., Farahani, H., Nuraei, R. (2024). *A novel linear algebra-based method for complex interval linear systems in circuit analysis*, *Heliyon* , 10, 1–12.

[12] Farahmand Nejad, M., Farahani, H., Nuraei, R., Gilani, A. (2014). *Gröbner basis approach for solving fuzzy complex system of linear equations*, *New Mathematics and Natural Computation* , 20 (2), 533–550.

[13] Faugère, J.-C. (1999). A new efficient algorithm for computing Gröbner bases (F_4). *Journal of Pure and Applied Algebra* , 139, 61–88.

[14] Faugère, J.-C. (2002). A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). Proceedings of ISSACS, T. Mora, Ed., ACM Press.

[15] Gamache, M., Hertz, A., Ouellet,J. O. (2007). *A graph coloring model for a feasibility problem in monthly crew scheduling with preferential bidding*, *Operations Research* , 34(8), 2384–2395.

[16] Gong, Z., Zhang, J. (2022). Chromatic Number of Fuzzy Graphs: Operations, Fuzzy Graph Coloring, and Applications. *Axioms* , 11 (12), DOI:10.3390/axioms11120697.

[17] Jafari, H., Farahani, H. (2024). Fuzzy Graph Coloring Using Gröbner Basis. *New Mathematics and Natural Computation* , 20 (2), 1–14.

[18] Kapur, D. (1986). *Using Gröbner Bases to Reason about Geometry Problems*, *Journal of Symbolic Computation* , 4, 399–408.

[19] Kubler, F., Renner, P., Schmedders, K. (2014). *Computing all solutions to polynomial equations in economics*, Elsevier.

[20] Lewis, R., Thompson, J. (2011). *On the application of graph coloring techniques in round robin*, *Computers & Operations Research* , 38(1), 190–204.

[21] Lin, Z. (2002). Gröbner bases and applications in control and systems. In 7th International Conference on Control, Automation, Robotics and Vision, ICARCV 2002, IEEE.

[22] Roanes-Lozano, E., Roanes-Macias, E., Laiti, L.M. (2004). *Some applications of Gröbner bases*, *Computing in Science & Engineering* , 6 (3), 56–60.

[23] Sturmfels, B. (1993). *Algorithms in Invariant Theory*, second edition, Springer.

[24] Wu, W.-T. (1994). *Mechanical Theorem Proving in Geometries: Basic Principles*, Springer-Verlag, 1994.